Available at www.MATHEMATICSweb.org
POWERED BY SCIENCE @ DIRECT®

ACADEMIC PRESS

JOURNAL OF Algebra

Journal of Algebra 261 (2003) 145–171

www.elsevier.com/locate/jalgebra

How long does it take to generate a group? ☆

Benjamin Klopsch [a,*] and Vsevolod F. Lev [b]

[a] *Mathematisches Institut, Heinrich-Heine-Universität, 40225 Düsseldorf, Germany*
[b] *Department of Mathematics, Haifa University at Oranim, Tivon 36006, Israel*

Received 6 February 2002

Communicated by Peter Littelmann

Abstract

The diameter of a finite group G with respect to a generating set A is the smallest non-negative integer n such that every element of G can be written as a product of at most n elements of $A \cup A^{-1}$. We denote this invariant by $\operatorname{diam}_A(G)$. It can be interpreted as the diameter of the Cayley graph induced by A on G and arises, for instance, in the context of efficient communication networks.

In this paper we study the diameters of a finite *Abelian* group G with respect to its various generating sets A. We determine the maximum possible value of $\operatorname{diam}_A(G)$ and classify all generating sets for which this maximum value is attained. Also, we determine the maximum possible cardinality of A subject to the condition that $\operatorname{diam}_A(G)$ is "not too small". Connections with caps, sum-free sets, and quasi-perfect codes are discussed.

1. Introduction

Let G be a finite group and let A be a subset of G. The *subgroup generated by A in G* is

$$\langle A\rangle := \bigcap\{H \leqslant G\colon\ A \subseteq H\},$$

the intersection of all subgroups containing A. This is the smallest subgroup of G lying above A. If $\langle A\rangle = G$ then A is called a *generating set for G*; so A generates G if and only

☆ At the time our collaboration started the first author held a PIMS postdoctoral fellowship at the University of Alberta (Canada) while the second author was a postdoctoral fellow at the Hebrew University of Jerusalem (Israel). We express our gratitude for the support provided by these institutions.

* Corresponding author.
E-mail addresses: klopsch@math.uni-duesseldorf.de (B. Klopsch), seva@math.haifa.ac.il (V.F. Lev).

0021-8693/03/$ – see front matter
doi:10.1016/S0021-8693(02)00671-3

if it is not contained in any proper subgroup of G. Loosely speaking, the aim of this paper is to determine whether and how quickly A generates G, using only information about the cardinality of A.

For this we regard generation as a dynamic step-by-step process. Since eventually we restrict to the situation where G is Abelian, we use additive notation throughout. Let $A^{\pm} := (-A) \cup \{0\} \cup A$ denote the "symmetric closure" of A with respect to addition. Thus $\langle A\rangle$ consists of all those $g \in G$ representable as a sum of elements of $A^{\pm}$, and for every non-negative integer ρ we define

$$\langle A\rangle_\rho := \rho A^{\pm} = \bigl\{a_1 + \cdots + a_\rho\colon\ a_i \in A^{\pm}\bigr\} \subseteq G,$$

the set of all $g \in G$ representable as a sum of *at most* ρ elements of $A^{\pm}$. Evidently, these sets form an ascending chain $\{0\} = \langle A\rangle_0 \subseteq \langle A\rangle_1 \subseteq \cdots$, and their union $\bigcup_{\rho \geqslant 0}\langle A\rangle_\rho = \langle A\rangle$ provides a bottom-up description of the subgroup generated by A. We notice that $\langle A^{\pm}\rangle_\rho = \langle A\rangle_\rho$ for every $\rho \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

We define the *diameter of G with respect to A* as

$$\mathrm{diam}_A(G) := \min\bigl\{\rho \in \mathbb{N}_0\colon\ \langle A\rangle_\rho = G\bigr\}.$$

To explain this nomenclature we introduce a suitable length function. For every $g \in G$ we define the *length of g with respect to A* as

$$l_A(g) := \min\bigl\{\rho \in \mathbb{N}_0\colon\ g \in \langle A\rangle_\rho\bigr\}.$$

Here we agree that $\min \varnothing = \infty$, so that for $g \in G$ we have $g \in \langle A\rangle$ if and only if $l_A(g) < \infty$. Observe that $l_A(g)$ is simply the minimum number of (not necessarily distinct) elements of $A^{\pm}$ required to represent g as their sum. Thus we have

$$\langle A\rangle_\rho = \bigl\{g \in G\colon\ l_A(g) \leqslant \rho\bigr\}$$

and

$$\mathrm{diam}_A(G) = \max\bigl\{l_A(g)\colon\ g \in G\bigr\}.$$

From this point of view the diameter allows a simple graph-theoretic interpretation. Indeed, $l_A(g)$ is the distance from zero to g in the Cayley graph induced by A on G, and $\mathrm{diam}_A(G)$ is the diameter of this graph. Moreover, $\mathrm{diam}_A(G)$ describes quantitatively "how long" it takes to generate G from A. In particular, A is a generating set for G if and only if $\mathrm{diam}_A(G) < \infty$.

The length of a given element and the diameter of G depend upon the choice of $A \subseteq G$. In contrast, the *absolute diameter*

$$\mathrm{diam}(G) := \max\bigl\{\mathrm{diam}_A(G)\colon\ \langle A\rangle = G\bigr\}$$

is an invariant of G itself: every generating set produces the group in at most that many steps.

The two problems addressed in this paper are:

P1. What is the value of $\operatorname{diam}(G)$ and what are the generating sets $A \subseteq G$ such that $\operatorname{diam}_A(G) = \operatorname{diam}(G)$?
P2. How large can $\operatorname{diam}_A(G)$ be, given that $|A|$ is large?

Under the assumption that G is *Abelian*, we solve the first problem completely (see Theorems 2.1 and 2.2) and we provide several partial answers to the second one (see Theorems 2.7, 2.9, and 2.12). Our results are presented in detail in the Section 2.

At first sight the restriction to Abelian groups may seem too strong—after all, finite Abelian groups are rather trivial objects from a group-theoretic point of view. But here we are concerned with combinatorial properties of finite groups, and already the case where G is homocyclic leads to interesting applications in coding theory and other areas; see Section 3.

Remark. Our starting point in this paper are representations of the elements of G by "algebraic sums" $\pm a_1 \pm \cdots \pm a_n$. However, it would be equally natural to allow only "pure sums" $a_1 + \cdots + a_n$. Formally, we could have put $A^+ := A \cup \{0\}$ and then proceeded to define $\langle A \rangle_\rho^+, \operatorname{diam}_A^+(G), l_A^+(g), \operatorname{diam}^+(G)$, etc. This approach leads to a significantly different theory, which we are going to cover in a separate paper.

Organization of the paper. In Sections 2 and 3 we describe our results in detail and place them into a broader context. Section 4 contains a list of auxiliary results. All proofs are collected in Sections 5–9.

Notation. The notation used is mostly standard, but the following list may be of help.

$\mathbb{N}$, $\mathbb{N}_0$, and $\mathbb{Z}$	the sets of positive, non-negative, and all integers, respectively.

For natural numbers $n, n_1, \ldots, n_r$:

$\mathbb{Z}_n$ (or $\mathbb{Z}/n\mathbb{Z}$)	the group of residues modulo n;
$\gcd(n_1, \ldots, n_r)$	the greatest common divisor of $n_1, \ldots, n_r$;
$\operatorname{lcm}(n_1, \ldots, n_r)$	the least common multiple of $n_1, \ldots, n_r$.

For real numbers x, y:

$\lfloor x \rfloor$	the greatest integer not exceeding x;
$\lceil x \rceil$	the smallest integer no smaller than x;
$[x, y]$	the set of all integers n satisfying $x \leqslant n \leqslant y$.

For a non-negative integer r and subsets $A, A_1, \ldots, A_r$ of an Abelian group G:

$A_1 + \cdots + A_r$	the set $\{a_1 + \cdots + a_r\colon a_1 \in A_1, \ldots, a_r \in A_r\}$;
rA	the set $A + \cdots + A$ (r summands);
$r * A$	the set $\{ra\colon a \in A\}$.

(For $r = 0$ the expressions $A_1 + \cdots + A_r$ and rA should be interpreted as $\{0\}$.)

Also, for integers m and n we write $m \mid n$ to indicate that m divides n.

2. Summary of results

We state our results in several blocks: first we look at the absolute diameter of a finite Abelian group and then at the maximum size of small diameter sets; cf. Problems P1 and P2 of Section 1.

2.1. The absolute diameter

Up to isomorphism, every finite Abelian group is completely characterized by its type. Let G be a finite Abelian group of type $(m_1, \ldots, m_r)$; that is, $G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ where $1 \neq m_1 \mid \cdots \mid m_r$. The number r is called the *rank of* G and denoted $\mathrm{rk}(G)$; it is the minimum number of elements required to generate G. A *standard generating set for* G is a subset $A = \{a_1, \ldots, a_r\} \subseteq G$ such that $G = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$ and $\mathrm{ord}(a_i) = m_i$ for all $i \in [1, r]$. It is worth pointing out that the trivial group $\{0\}$ has type $()$, rank 0, and precisely one standard generating set, namely $\varnothing$.

Perhaps not surprisingly, the diameter of G with respect to a standard generating set is as large as possible. Indeed, if A is a standard generating set for G, then plainly $\mathrm{diam}_A(G) = \sum_{i=1}^{r} \lfloor m_i/2 \rfloor$, and we establish

Theorem 2.1. *A finite Abelian group G of type $(m_1, \ldots, m_r)$ has diameter*

$$\mathrm{diam}(G) = \sum_{i=1}^{r} \lfloor m_i/2 \rfloor.$$

Conversely, if A is a generating set for G with $\mathrm{diam}_A(G) = \mathrm{diam}(G)$, then A is "nearly standard"; a small wrinkle is observed if G has invariant factors of order three. To make this precise, for $m \in \mathbb{N}$ we define

$$\nu_m(G) := \#\{i \in [1, r]\colon\ m_i = m\}, \tag{2.1}$$

the number of components of $(m_1, \ldots, m_r)$ equal to m. We notice that, if m is prime and $\nu_m(G) \neq 0$, then $m_i = m$ for all $i \in [1, \nu_m(G)]$. Furthermore, if m' and m'' are co-prime, then at least one of $\nu_{m'}(G)$ and $\nu_{m''}(G)$ is zero.

Theorem 2.2. *Let G be a finite Abelian group of rank r. Then for every subset $A \subseteq G$ the following assertions are equivalent*:

(i) $\mathrm{diam}_A(G) = \mathrm{diam}(G)$;

(ii) *there exists a standard generating set $B = \{b_1, \ldots, b_r\}$ for G such that*

$$B^{\pm} \subseteq A^{\pm} \subseteq \bigl(B \cup \bigl\{b_{2i-1} + b_{2i}\colon\ i \in [1, \nu_3(G)/2]\bigr\}\bigr)^{\pm}.$$

Corollary 2.3. *Let G be a finite Abelian group. Then for every subset $A \subseteq G$ satisfying $\mathrm{diam}_A(G) = \mathrm{diam}(G)$ we have*

$$\mathrm{rk}(G) \leqslant |A| \leqslant 1 + 2\,\mathrm{rk}(G) - \nu_2(G) + 2\lfloor \nu_3(G)/2 \rfloor.$$

Indeed, both bounds are sharp.

For Abelian groups these theorems provide a complete solution to Problem P1 of Section 1. In contrast, for no infinite family $\mathcal{H}$ of non-Abelian finite groups such explicit formulae for the diameters $\mathrm{diam}(H)$, $H \in \mathcal{H}$, seem to be known.

2.2. The maximum size of small diameter sets: definitions

Let G be a finite Abelian group. Intuitively, it is clear that the larger a subset $A \subseteq G$, the smaller the corresponding diameter $\mathrm{diam}_A(G)$. But to what extent does the size of A alone guarantee fast generation?

Suppose that $\rho \in \mathbb{N}$. We want to find an upper bound for the sizes of generating sets A for G with $\mathrm{diam}_A(G) \geqslant \rho$. Agreeing that $\max \varnothing = 0$, we define

$$\mathbf{s}_\rho(G) := \max\bigl\{|A|\colon\ A \subseteq G \text{ such that } \rho \leqslant \mathrm{diam}_A(G) < \infty\bigr\}.$$

Equivalently, we have $\mathbf{s}_\rho(G) = \max\{|A|\colon\ A \subseteq G \text{ such that } \langle A\rangle_{\rho-1} \neq \langle A\rangle = G\}$. The significance of this new invariant stems from the observation that every generating set A for G of size larger than $\mathbf{s}_\rho(G)$ surely generates G in less than ρ steps.

In order to better understand $\mathbf{s}_\rho(G)$ we introduce a related and perhaps more fundamental invariant, $\mathbf{t}_\rho(G)$; this requires a short preparation. Recall that the *period* of a subset $S \subseteq G$ is the subgroup $\pi(S) := \{g \in G\colon\ S + g = S\} \leqslant G$, and S is *periodic* or *aperiodic* according to whether $\pi(S) \neq \{0\}$ or $\pi(S) = \{0\}$. Clearly, S is a union of $\pi(S)$-cosets; consequently, if $\gcd(|S|, |G|) = 1$ then S is aperiodic. Another useful observation is that the image of S under the canonical homomorphism $G \to G/\pi(S)$ is an aperiodic subset of the quotient group $G/\pi(S)$.

We say that a subset $A \subseteq G$ is ρ-*maximal* if it is maximal (under inclusion) subject to $\mathrm{diam}_A(G) \geqslant \rho$; that is, subject to $\langle A\rangle_{\rho-1} \neq G$. Plainly, we have

$$\mathbf{s}_\rho(G) = \max\bigl\{|A|\colon\ A \text{ is a } \rho\text{-maximal generating set for } G\bigr\}.$$

One can construct ρ-maximal generating sets by a “lifting process” as follows. Suppose that $H \lneqq G$, and let $\varphi\colon G \to G/H$ denote the canonical homomorphism. If $\overline{A} = \overline{A}^{\,\pm}$ is a generating set for G/H, then the full pre-image $A := \varphi^{-1}(\overline{A})$ is a generating set for G with $\mathrm{diam}_A(G) = \mathrm{diam}_{\overline{A}}(G/H)$ and $\pi(A) \geqslant H$. Conversely, suppose $A = A^{\pm}$ is a generating set for G and $H \leqslant \pi(A)$. Then the image $\overline{A} = \varphi(A)$ is a generating set for G/H and $\mathrm{diam}_{\overline{A}}(G/H) = \mathrm{diam}_A(G)$. Furthermore, if A is ρ-maximal then so is $\overline{A}$, and if $H = \pi(A)$ then $\overline{A}$ is aperiodic. This shows that every ρ-maximal generating set is induced by an aperiodic one. A natural point of view, therefore, is to consider *aperiodic* ρ-maximal generating sets as "primitive" and concentrate on their properties first. Accordingly, we let

$$\mathbf{t}_\rho(G) := \max\bigl\{|A|:\ A \text{ is an aperiodic } \rho\text{-maximal generating set for } G\bigr\},$$

again subject to the agreement that $\max\varnothing = 0$.

We notice that, if $\rho > \operatorname{diam}(G)$, then $\rho > \operatorname{diam}_A(G)$ for all generating subsets $A \subseteq G$; consequently, G admits no ρ-maximal generating sets and $\mathbf{t}_\rho(G) = 0$. On the other hand, if $\rho \in [1, \operatorname{diam}(G)]$ then in the definition of $\mathbf{t}_\rho(G)$ we can safely disregard the requirement that A generates G. Indeed, suppose that $A \subseteq G$ is ρ-maximal, but does not generate G. Then A is a proper subgroup of G. Suppose that in addition A is aperiodic. Then $A = \{0\}$ lies in the symmetric closure $B^{\pm}$ of every subset $B \subseteq G$; it follows that $\operatorname{diam}(G) < \rho$. In summary, we have

$$\mathbf{t}_\rho(G) = \begin{cases} \max\bigl\{|A|:\ A \subseteq G \text{ is aperiodic and } \rho\text{-maximal}\bigr\} & \text{if } \rho \in [1, \operatorname{diam}(G)],\\ 0 & \text{if } \rho > \operatorname{diam}(G). \end{cases}$$

The close connection between $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$ is described by

Lemma 2.4. *Let G be a finite Abelian group and let $\rho \in [2, \operatorname{diam}(G)]$. Then*

$$\mathbf{s}_\rho(G) = \max\bigl\{|H| \cdot \mathbf{t}_\rho(G/H):\ H \lneqq G\bigr\}.$$

Unless G is trivial, the only 1-maximal subset of G is G itself; so $\mathbf{s}_1(G) = |G|$ and $\mathbf{t}_1(G) = 0$. In fact, it can happen that $\mathbf{t}_\rho(G) = 0$ also for $\rho \in [2, \operatorname{diam}(G)]$. Examples of this kind can be constructed as follows.

Example 2.5. *Let $n \in \mathbb{N}$ with $n \geqslant 2$, and let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n+1}}$. Then $\operatorname{diam}(G) = 1 + 2^n$, and every 2^n-maximal subset of G is periodic.*

Perhaps it is feasible to classify all pairs (G, ρ) such that $\mathbf{t}_\rho(G) = 0$, but beyond Example 2.5 nothing much is known.

2.3. The maximum size of small diameter sets: explicit formulae

We completely determine $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$ in the following particular cases:

(i) G is an arbitrary finite Abelian group and $\rho \in \{1, 2, 3, \operatorname{diam}(G)\}$;
(ii) G is a finite cyclic group and $\rho \in [1, \operatorname{diam}(G)]$ is arbitrary.

The case $\rho = 1$ is settled by the observation preceding Example 2.5. The case $\rho = 2$ is not difficult either.

Proposition 2.6. *Let G be a finite Abelian group with $\operatorname{diam}(G) \geqslant 2$. Then*

$$\mathbf{t}_2(G) = \mathbf{s}_2(G) = \begin{cases} |G| - 1 & \text{if } |G| \text{ is even},\\ |G| - 2 & \text{if } |G| \text{ is odd}. \end{cases}$$

For the next theorem recall that the *exponent* of an Abelian group G is $\exp(G) = \max\{\mathrm{ord}(g)\colon g \in G\}$, where $\mathrm{ord}(g)$ denotes the order of $g \in G$. The 2-*rank* of G, denoted $\mathrm{rk}_2(G)$, is the rank of the Sylow 2-subgroup of G. The group G is called *homocyclic* if it can be written as a direct sum of pairwise isomorphic cyclic groups.

Suppose that G is of type $(m_1, \ldots, m_r)$. Then we have $\mathrm{rk}(G) = r$ and, unless G is trivial, $\exp(G) = m_r$. Moreover, $\mathrm{rk}_2(G)$ is the number of indices $i \in [1, r]$ for which m_i is even, and $\mathrm{rk}_2(2 * G)$ is the number of indices $i \in [1, r]$ for which m_i is divisible by four. (Here $2 * G$ denotes the set $\{2g\colon g \in G\}$; see our list of definitions at the end of Section 1.) Clearly, G is homocyclic if and only if $m_1 = \cdots = m_r$.

Theorem 2.7. *Let G be a finite Abelian group with* $\mathrm{diam}(G) \geqslant 3$.

(i) *Suppose that $|G|$ is odd, and let $n := \exp(G)$. Then*

$$\mathbf{t}_3(G) = \mathbf{s}_3(G) = \begin{cases} \dfrac{n-1}{2n}|G| - 1 & \text{if } n \equiv 1 \pmod 4, \\ \dfrac{n-1}{2n}|G| & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(ii) *Suppose that $|G|$ is even. Then*

$$\mathbf{t}_3(G) = \begin{cases} \bigl(|G| - \sqrt{|G|}\bigr)/2 & \text{if } G \text{ is homocyclic of exponent } 4, \\ |G|/2 - 1 & \text{if } \mathrm{rk}_2(G) = \mathrm{rk}_2(2 * G) \text{ and } \exp(G) > 4, \\ |G|/2 & \text{if } \mathrm{rk}_2(G) > \mathrm{rk}_2(2 * G), \end{cases}$$

$$\mathbf{s}_3(G) = \begin{cases} |G|/2 - 1 & \text{if } G \text{ is a cyclic } 2\text{-group}, \\ |G|/2 & \text{otherwise.} \end{cases}$$

The proof of this theorem already requires a fair amount of work. Probably, it will be significantly more difficult to find explicit formulae for $\mathbf{t}_4(G)$ and $\mathbf{s}_4(G)$. Some general estimates are given later in this section.

Our next result is a consequence of Theorem 2.2; see also Corollary 2.3.

Corollary 2.8. *Let G be a finite Abelian group, and suppose that $\rho := \mathrm{diam}(G) \geqslant 2$. Then*

$$\mathbf{t}_\rho(G) = \mathbf{s}_\rho(G) = 1 + 2\,\mathrm{rk}(G) - \nu_2(G) + 2\lfloor \nu_3(G)/2 \rfloor.$$

We now turn our attention towards cyclic groups. Notice that $\mathrm{diam}(\mathbb{Z}_m) = \lfloor m/2 \rfloor$ for all $m \in \mathbb{N}$, by Theorem 2.1.

Theorem 2.9. *Let $m \in \mathbb{N}$ and $\rho \in [2, m/2]$. Then*

$$\mathbf{t}_\rho(\mathbb{Z}_m) = 2\left\lfloor \frac{m-2}{2(\rho-1)} \right\rfloor + 1$$

and

$$\mathbf{s}_\rho(\mathbb{Z}_m) = \max\left\{\frac{m}{d}\left(2\left\lfloor\frac{d-2}{2(\rho-1)}\right\rfloor + 1\right): d \mid m,\ d \geqslant 2\rho\right\}.$$

In particular, for cyclic groups of prime order this reduces to

Corollary 2.10. *Let $p \geqslant 5$ be a prime and suppose that $\rho \in [2, (p-1)/2]$. Then*

$$\mathbf{t}_\rho(\mathbb{Z}_p) = \mathbf{s}_\rho(\mathbb{Z}_p) = 2\left\lfloor\frac{p-2}{2(\rho-1)}\right\rfloor + 1.$$

2.4. The maximum size of small diameter sets: estimates

Let G be a finite Abelian group and let $\rho \in [1, \operatorname{diam}(G)]$. For $\rho \geqslant 4$ the exact values of $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$ are likely to depend—in an increasingly complicated way—on the algebraic structure of G. Nevertheless, some general estimates in terms of ρ and $|G|$ can be given. To some extent such estimates compensate for the lack of explicit formulae as those we were able to provide for $\rho \leqslant 3$. Moreover, the bounds given by the following proposition are used in the proofs of several of the results stated above.

Proposition 2.11. *Let G be a finite Abelian group, and suppose that $\rho \geqslant 2$. Then*

$$\mathbf{t}_\rho(G) \leqslant \left\lfloor\frac{|G|-2}{\rho-1}\right\rfloor + 1.$$

Moreover, if $\operatorname{rk}_2(G) \leqslant 1$ *then*

$$\mathbf{t}_\rho(G) \leqslant 2\left\lfloor\frac{|G|-2}{2(\rho-1)}\right\rfloor + 1.$$

Our two final results provide further bounds.

Theorem 2.12. *Let G be a finite Abelian group, and suppose that $\rho \geqslant 4$. Then $\mathbf{s}_\rho(G) \leqslant \frac{3}{2}\rho^{-1}|G|$, and equality holds if and only if G has a subgroup H such that G/H is cyclic of order 2ρ. Indeed, the following assertions are equivalent*:

(i) *A is a generating set for G satisfying* $\operatorname{diam}_A(G) \geqslant \rho$ *and* $|A| = \frac{3}{2}\rho^{-1}|G|$;
(ii) *$A = (-g+H) \cup H \cup (g+H)$, where H is a subgroup of G such that G/H is cyclic of order 2ρ, and g is an element of G such that $g+H$ is a generator of G/H.*

This theorem shows that the maximum possible cardinality of a generating set A with $\operatorname{diam}_A(G) \geqslant \rho$ is $\frac{3}{2}\rho^{-1}|G|$ and it describes the structure of all A with precisely this cardinality. Our next result goes beyond this, establishing the structure of those generating sets A with $\operatorname{diam}_A(G) \geqslant \rho$ and $|A^{\pm}| > (4/(3\rho-1))|G|$.

Theorem 2.13. *Let G be a finite Abelian group, and suppose that $\rho \geqslant 4$. If A is a generating set for G such that* $\operatorname{diam}_A(G) \geqslant \rho$ *and* $|A^{\pm}| > 4|G|/(3\rho - 1)$, *then there exist* $H \leqslant G$ *and* $g \in G$ *satisfying the following conditions*:

(i) $A \subseteq (-g + H) \cup H \cup (g + H)$, *and* $|A^{\pm}| > (3 - (\rho - 3)/(3\rho - 1))|H|$;
(ii) G/H *is cyclic of order* $2\rho \leqslant |G/H| \leqslant \frac{9}{4}\rho - 1$, *and* $g + H$ *generates* G/H.

3. Context and motivation

As far as we know, diameters of finite groups have never been studied systematically. Nevertheless, many individual problems have been considered and to a certain extent solved. We provide several selected examples, mainly to illustrate the various interconnections with other areas of research.

A lot of attention has been given to homocyclic groups of exponent 2, that is, groups isomorphic to $\mathbb{Z}_2^r$ for some $r \in \mathbb{N}_0$. There are at least three good reasons for this.

(i) *Connections with the covering radius in coding theory.* There is a natural correspondence between generating sets A for $\mathbb{Z}_2^r$ and linear binary block codes of co-dimension r and minimum distance $d \geqslant 3$. (Given such a set A, one can arrange its non-zero elements in columns to obtain a check matrix of the code associated to A. For more details, see [4, Section 18.1] or [5].) The length of the code corresponding to A is $|A \setminus \{0\}|$ and its covering radius is $\operatorname{diam}_A(\mathbb{Z}_2^r)$. This shows that codes of minimum distance $d \geqslant 3$, co-dimension r, and covering radius at least ρ exist if and only if $\rho \in [1, r]$; in this case the maximum possible length of such a code is $\mathbf{s}_\rho(\mathbb{Z}_2^r) - 1$.

(ii) *Connections with caps in projective geometries.* A cap in a projective geometry is a collection of points no three of which are collinear. In a finite projective geometry $\mathrm{PG}(r - 1, 2)$ over the field with two elements, points can be identified with the non-zero elements of $\mathbb{Z}_2^r$, and then caps correspond to subsets $A \subseteq \mathbb{Z}_2^r \setminus \{0\}$ such that no three elements of A add up to zero. Evidently, if A is a cap, then for any $a \in A$ we have $a \notin \langle A + a\rangle_3$, whence $\operatorname{diam}_{A+a}(\mathbb{Z}_2^r) \geqslant 4$; moreover, if A is not contained in a hyperplane of $\mathrm{PG}(r-1, 2)$, then $A + a$ generates $\mathbb{Z}_2^r$. Conversely, suppose that B is a generating set for $\mathbb{Z}_2^r$ such that $\operatorname{diam}_B(\mathbb{Z}_2^r) \geqslant 4$ and $0 \in B$. Then for any $g \in \mathbb{Z}_2^r \setminus \langle B\rangle_3$ the set $A := B + g$ is a cap, not contained in a hyperplane. Therefore the maximum size of a cap, not contained in a hyperplane, is $\mathbf{s}_4(\mathbb{Z}_2^r)$. For (much) more on caps we refer the reader to [2,7].

(iii) *Connections with sum-free sets in combinatorial number theory.* A subset $A \subseteq G$ of an Abelian group G is said to be sum-free if no two elements of A add up to another element of A. For $G = \mathbb{Z}_2^r$ this reduces to $a_1 + a_2 + a_3 \neq 0$ for all $a_1, a_2, a_3 \in A$. As shown above, sets with this property are translates of sets of diameter greater than three. Thus the maximum size of a sum-free subset of $\mathbb{Z}_2^r$, not contained in any coset of any proper subgroup, is $\mathbf{s}_4(\mathbb{Z}_2^r)$. More information on sum-free subsets of $\mathbb{Z}_2^r$ can be found in [3].

The remarks in (i) and (iii) lead to further connections with coding theory: it is not difficult to see that the code C, corresponding to a maximal (under inclusion) sum-free subset of $\mathbb{Z}_2^r$, has minimum distance $d \in \{4, 5\}$ and covering radius $\rho = 2$. If $d = 5$, then C is a perfect code; in fact, it is known that the only code with $d = 5$ and $\rho = 2$ is the repetition code of length 5, which has co-dimension $r = 4$. For $r > 4$ we necessarily have $d = 4$, and C is a quasi-perfect code. Thus $\mathbf{s}_4(\mathbb{Z}_2^r)$ can be interpreted as the maximum length of a "non-trivial" quasi-perfect code of co-dimension r and covering radius $\rho = 2$. ("Trivial" quasi-perfect codes correspond to sum-free sets that are complements of index two subgroups. These codes are extensions of the Hamming codes.)

In their remarkable paper [6], Davydov and Tombak have shown that

$$\mathbf{t}_4\big(\mathbb{Z}_2^r\big) = 2^{r-2} + 1 \quad \text{and} \quad \mathbf{s}_4\big(\mathbb{Z}_2^r\big) = 5 \cdot 2^{r-4} \tag{3.1}$$

for $r \geqslant 4$. We note that the first of these equalities is much subtler than the second one. Indeed, the value of $\mathbf{s}_4(\mathbb{Z}_2^r)$ was re-established independently by other authors [2,3], whereas—to our knowledge—no alternative proof of the formula for $\mathbf{t}_4(\mathbb{Z}_2^r)$ has been found. Using the first of Equations (3.1), Davydov and Tombak were able to treat several related problems; for instance, they found all possible lengths $n \geqslant 2^{r-1} + 1$ of quasi-perfect codes of co-dimension r and covering radius $\rho = 2$.

For $\rho \geqslant 5$, until recently only estimates and no precise formulae for $\mathbf{s}_\rho(\mathbb{Z}_2^r)$ were known; see [5,13] or [4, Chapter 18]. The exact values are determined in a forthcoming paper by one of the present authors [11]. Concerning general bounds we mention that [8, Lemma 3] can be regarded as a precursor of our Theorem 2.12: in our notation, it asserts that

$$\operatorname{diam}_A(G) \leqslant \max\left\{2, \frac{3|G|}{2|A|}\right\}$$

for every generating set A of a finite Abelian group G.

It is worth pointing out that there are also investigations of the diameters of non-Abelian finite simple groups. Apart from the 26 so-called sporadic isomorphism classes, non-Abelian finite simple groups are known to fall into two categories: they are either alternating or of Lie type. In the survey [1] one finds a discussion of three types of generating sets for these groups: "worst" (giving maximal diameter), "average" (a random choice of a prescribed number of generators) and "best" (giving minimal diameter while keeping the number of generators limited). Instead of precise formulae the authors describe asymptotic bounds, as the group order tends to infinity. One of the important, as yet unproven conjectures [1, Section 2] states that for non-Abelian finite simple groups G, one has $\operatorname{diam}(G) = (\log|G|)^{O(1)}$ as $|G| \to \infty$.

4. Auxiliary results

For later use we list three well-known results about Abelian groups. The first two are very basic lemmata, which will be used freely without further reference.

Lemma 4.1. *If $\{g_1, \ldots, g_r\}$ is a generating set for a finite Abelian group G, then* $\exp(G) = \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_r)))$.

Lemma 4.2. *If G is a finite Abelian group and $g \in G$ has order* $\operatorname{ord}(g) = \exp(G)$, *then there exists a subgroup $H \leqslant G$ such that $G = H \oplus \langle g \rangle$.*

The next result is a much deeper theorem due to Kneser.

Theorem 4.3 (Kneser [9,10]; see also [12]). *Let A and B be finite non-empty subsets of an Abelian group G such that*

$$|A + B| \leqslant |A| + |B| - 1.$$

Then, letting $H := \pi(A + B)$, we have

$$|A + B| = |A + H| + |B + H| - |H|.$$

Since, in the above notation, we have $|A + H| \geqslant |A|$ and $|B + H| \geqslant |B|$, Theorem 4.3 shows that $|A + B| \geqslant |A| + |B| - |H|$. A straightforward induction yields

Corollary 4.4. *Let $A_1, \ldots, A_r$ be finite non-empty subsets of an Abelian group G, and write $H := \pi(A_1 + \cdots + A_r)$. Then we have*

$$|A_1 + \cdots + A_r| \geqslant |A_1| + \cdots + |A_r| - (r-1)|H|.$$

In particular, if $A_1 + \cdots + A_r$ is aperiodic, then

$$|A_1 + \cdots + A_r| \geqslant |A_1| + \cdots + |A_r| - (r-1).$$

In fact, Theorem 4.3 and Corollary 4.4 are equivalent, as the former can easily be derived from the latter. For this reason we often refer to Corollary 4.4 simply as “Kneser’s theorem”.

5. The absolute diameter

In this section we establish Theorem 2.1, Theorem 2.2, and Corollary 2.3 after proving some subsidiary results.

Lemma 5.1. *Let $G = G_1 \oplus \cdots \oplus G_r$ be a finite Abelian group, and let $A = A_1 \cup \cdots \cup A_r$ where $A_i \subseteq G_i$ for all $i \in [1, r]$. Then*

$$\operatorname{diam}_A(G) = \operatorname{diam}_{A_1}(G_1) + \cdots + \operatorname{diam}_{A_r}(G_r).$$

Proof. Given $g = g_1 + \cdots + g_r \in G$, with $g_i \in G_i$ for all $i \in [1, r]$, we have

$$l_A(g) = l_{A_1}(g_1) + \cdots + l_{A_r}(g_r),$$

and the assertion follows. □

Lemma 5.2. *Let $n_1, \dots, n_r \in \mathbb{N}$ where $r \geqslant 2$. Suppose that for every $i \in [1, r]$ we have*

$$\operatorname{lcm}(n_1, \dots, n_r) > \operatorname{lcm}(n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_r).$$

Then

$$\operatorname{lcm}(n_1, \dots, n_r) \geqslant 2^{r-1} \max\{n_i \colon i \in [1, r]\}.$$

Consequently,

$$\operatorname{lcm}(n_1, \dots, n_r) > n_1 + \cdots + n_r$$

and

$$\left\lfloor \frac{\operatorname{lcm}(n_1, \dots, n_r)}{2} \right\rfloor > \left\lfloor \frac{n_1}{2} \right\rfloor + \cdots + \left\lfloor \frac{n_r}{2} \right\rfloor.$$

Proof. Without loss of generality we can assume that $\max\{n_i \colon i \in [1, r]\} = n_1$. Since $\operatorname{lcm}(n_1, \dots, n_i)$ is a proper divisor of $\operatorname{lcm}(n_1, \dots, n_{i+1})$ for every $i \in [1, r-1]$, we have

$$\operatorname{lcm}(n_1, \dots, n_r) \geqslant 2 \operatorname{lcm}(n_1, \dots, n_{r-1}) \geqslant 4 \operatorname{lcm}(n_1, \dots, n_{r-2}) \geqslant \cdots \geqslant 2^{r-1} n_1.$$

Next, as $2^{r-1} \geqslant r$, we obtain $\operatorname{lcm}(n_1, \dots, n_r) > n_1 + \cdots + n_r$. For the last assertion we note that, if $\operatorname{lcm}(n_1, \dots, n_r)$ is odd, then so are all of $n_1, \dots, n_r$. $\square$

Proof of Theorem 2.1. Suppose that $G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ where $1 \neq m_1 \mid \cdots \mid m_r$. Considering standard generating sets we already observed that $\operatorname{diam}(G) \geqslant \lfloor m_1/2 \rfloor + \cdots + \lfloor m_r/2 \rfloor$. It remains to establish the reverse inequality.

Let A be a generating set for G, and let $g \in G$. We use induction on r to verify that

$$l_A(g) \leqslant \lfloor m_1/2 \rfloor + \cdots + \lfloor m_r/2 \rfloor. \tag{5.1}$$

For $r = 0$ there is nothing to prove, and we assume that $r \geqslant 1$. Put $s := |A|$ and write $A = \{a_1, \dots, a_s\}$. Renumbering the elements of A, if necessary, we find $t \in [1, s]$ such that

(i) the group $\langle a_t, a_{t+1}, \dots, a_s \rangle$ contains an element a of order $\operatorname{ord}(a) = m_r$;
(ii) for every $i \in [t, s]$ the group $\langle a_t, \dots, a_{i-1}, a_{i+1}, \dots, a_s \rangle$ does not contain any elements of order m_r.

For later use we note that these conditions are equivalent to

(I) $\operatorname{lcm}(\operatorname{ord}(a_t), \dots, \operatorname{ord}(a_s)) = m_r$;
(II) $\operatorname{lcm}(\operatorname{ord}(a_t), \dots, \operatorname{ord}(a_{i-1}), \operatorname{ord}(a_{i+1}), \dots, \operatorname{ord}(a_s)) < m_r$ for all $i \in [t, s]$.

Regarding the interpretation of conditions (ii) and (II) for $t = s$ we notice that $\langle\varnothing\rangle = \{0\}$ and $\operatorname{lcm}(\varnothing) = 1$, in accordance with standard definitions.

We find a subgroup $H \leqslant G$ such that $G = H \oplus \langle a\rangle$ and $H \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_{r-1}}$. Let $\beta_1, \ldots, \beta_s \in \mathbb{Z}$ such that $b_i := a_i + \beta_i a \in H$ for all $i \in [1, s]$.

We note that $H = \langle b_1, \ldots, b_s\rangle$. Indeed, given $h \in H$ we find $\lambda_1, \ldots, \lambda_s \in \mathbb{Z}$ such that

$$h = \sum_{i=1}^{s} \lambda_i a_i = \sum_{i=1}^{s} \lambda_i (b_i - \beta_i a) = \sum_{i=1}^{s} \lambda_i b_i - \left(\sum_{i=1}^{s} \lambda_i \beta_i\right) a,$$

and $G = H \oplus \langle a\rangle$ implies that $h = \sum_{i=1}^{s} \lambda_i b_i \in \langle b_1, \ldots, b_s\rangle$.

Now we are ready to prove (5.1). We find $h \in H$ and $\nu \in \mathbb{Z}$ such that $g = h + \nu a$. By the induction hypothesis, there are $\lambda_1, \ldots, \lambda_s \in \mathbb{Z}$ such that $h = \sum_{i=1}^{s} \lambda_i b_i$ and $\sum_{i=1}^{s} |\lambda_i| \leqslant \sum_{i=1}^{r-1} \lfloor m_i/2\rfloor$. By (i), there exist $\mu_t, \ldots, \mu_s \in \mathbb{Z}$ with $|\mu_i| \leqslant \lfloor \operatorname{ord}(a_i)/2\rfloor$ for $i \in [t, s]$ so that

$$g = \sum_{i=1}^{s} \lambda_i b_i + \nu a = \sum_{i=1}^{s} \lambda_i a_i + \left(\nu + \sum_{i=1}^{s} \lambda_i \beta_i\right) a = \sum_{i=1}^{t-1} \lambda_i a_i + \sum_{i=t}^{s} \mu_i a_i.$$

Recalling (I) and (II), we apply Lemma 5.2 to find

$$l_A(g) \leqslant \sum_{i=1}^{t-1} |\lambda_i| + \sum_{i=t}^{s} |\mu_i| \leqslant \sum_{i=1}^{r-1} \lfloor m_i/2\rfloor + \sum_{i=t}^{s} \lfloor \operatorname{ord}(a_i)/2\rfloor \leqslant \sum_{i=1}^{r} \lfloor m_i/2\rfloor,$$

as required. □

Lemma 5.3. *Let G be a finite Abelian group, and suppose that $A \subseteq G$ is minimal* (*under inclusion*) *subject to* $\operatorname{diam}_A(G) = \operatorname{diam}(G)$. *Then A is a standard generating set.*

Proof. Suppose that G has type $(m_1, \ldots, m_r)$, that is $G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ where $1 \neq m_1 \mid \cdots \mid m_r$. We use induction on r.

The case $r = 0$ is trivial and we assume that $r \geqslant 1$. Revisit the proof of Theorem 2.1; write $A = \{a_1, \ldots, a_s\}$ and define t as before. Following the original argument (while keeping in mind that the last inequality in Lemma 5.2 is strict), the equation $\operatorname{diam}_A(G) = \operatorname{diam}(G) = \sum_{i=1}^{r} \lfloor m_i/2\rfloor$ now shows that $t = s$, so $\operatorname{ord}(a_s) = m_r$.

As in the proof of Theorem 2.1, we find $H \leqslant G$ such that $G = H \oplus \langle a_s\rangle$, and consequently $H \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_{r-1}}$. Furthermore, for every $i \in [1, s-1]$ we find $\beta_i \in \mathbb{Z}$ such that $b_i := a_i + \beta_i a_s \in H$. By minimality of A, we have $b_i \neq 0$, and $b_i \neq b_j$ (unless $i = j$) for all $i, j \in [1, s-1]$.

It is easily seen that $B := \{b_1, \ldots, b_{s-1}\}$ satisfies $\operatorname{diam}_B(H) = \sum_{i=1}^{r-1} \lfloor m_i/2\rfloor = \operatorname{diam}(H)$ and is minimal subject to this condition. By the induction hypothesis, B is a standard generating set for H. This yields $s = r$,

$$G = H \oplus \langle a_r\rangle = \langle b_1\rangle \oplus \cdots \oplus \langle b_{r-1}\rangle \oplus \langle a_r\rangle$$

and without loss of generality we may assume that $\operatorname{ord}(b_j) = m_j$ for all $j \in [1, r-1]$.

To show that A is a standard generating set for G, it is enough to prove that $\operatorname{ord}(a_j) \mid m_j$, or equivalently

$$m_r \mid m_j \beta_j \tag{5.2}$$

for all $j \in [1, r-1]$.

For a contradiction, suppose that $j \in [1, r-1]$ is an index for which (5.2) fails. Fix $g \in G$ such that $l_A(g) = \operatorname{diam}(G)$ and write $g = \lambda_1 b_1 + \cdots + \lambda_{r-1} b_{r-1} + \lambda a_r$, with $-m_i/2 < \lambda_i \leqslant m_i/2$ for $i \in [1, r-1]$. Substituting $b_i = a_i + \beta_i a_r$ we get $g = \lambda_1 a_1 + \cdots + \lambda_{r-1} a_{r-1} + \lambda_r a_r$ with $-m_r/2 < \lambda_r \leqslant m_r/2$. As $l_A(g) = \sum_{i=1}^r \lfloor m_i/2 \rfloor$, we actually have $|\lambda_i| = \lfloor m_i/2 \rfloor$ for all $i \in [1, r]$. Define

$$\varepsilon := \begin{cases} 0 & \text{if } \lambda_j = m_j/2, \\ 1 & \text{if } \lambda_j = (m_j - 1)/2, \\ -1 & \text{if } \lambda_j = -(m_j - 1)/2. \end{cases}$$

and

$$\mu_i := \begin{cases} \lambda_i & \text{if } i \in [1, r-1], i \neq j, \\ -\lambda_j - \varepsilon & \text{if } i = j. \end{cases}$$

Furthermore, choose $\mu_r \in \mathbb{Z}$ such that $|\mu_r| \leqslant \lfloor m_r/2 \rfloor$ and $\mu_r \equiv \lambda_r + (\mu_j - \lambda_j)\beta_j \pmod{m_r}$.

Notice that $|\mu_j| = |\lambda_j| + |\varepsilon|$ and $\mu_j \equiv \lambda_j \pmod{m_j}$. The latter relation implies

$$\mu_j a_j + \mu_r a_r = \mu_j (b_j - \beta_j a_r) + (\lambda_r + (\mu_j - \lambda_j)\beta_j) a_r = \lambda_j a_j + \lambda_r a_r,$$

and hence $g = \mu_1 a_1 + \cdots + \mu_r a_r$.

Moreover, $\mu_r \equiv \lambda_r - m_j \beta_j \pmod{m_r}$ if $\varepsilon = 0$, and $\mu_r \equiv \lambda_r - \varepsilon m_j \beta_j \pmod{m_r}$ otherwise. From the fact that m_j is a proper divisor of m_r and $m_r \nmid m_j \beta_j$, it is not difficult to derive that $|\mu_r| \leqslant |\lambda_r| - m_j + 1$. Thus $|\mu_j| + |\mu_r| \leqslant |\lambda_j| + |\varepsilon| + |\lambda_r| - m_j + 1 < |\lambda_j| + |\lambda_r|$.

Therefore we obtain $g = \mu_1 a_1 + \cdots + \mu_r a_r$ where $\sum_{i=1}^r |\mu_i| < \sum_{i=1}^r |\lambda_i| = l_A(g)$, a contradiction, as required. □

Lemma 5.4. (i) *Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and put $A := \{(1,0), (0,1), (1,1)\}^{\pm}$. Then A satisfies* $\operatorname{diam}_A(G) = \operatorname{diam}(G)$ *and is maximal* (*under inclusion*) *subject to this condition.*

(ii) *Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and put $A := \{(1,0,0), (0,1,0), (0,0,1), (1, \varepsilon_1, 0), (1, 0, \varepsilon_2)\}^{\pm}$, where $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$. Then* $\operatorname{diam}_A(G) < \operatorname{diam}(G)$.

Proof. (i) Theorem 2.1 shows that $\operatorname{diam}(G) = 2$, and the claim follows easily from $A = G \setminus \{(1,-1), (-1,1)\}$.

(ii) Theorem 2.1 shows that $\operatorname{diam}(G) = 3$. Applying an automorphism of G if necessary, we may assume without loss of generality that $\varepsilon_1 = \varepsilon_2 = 1$. Now it is easy to check that $\operatorname{diam}_A(G) = 2$. □

Proof of Theorem 2.2. Let $A \subseteq G$. If $\langle A\rangle \neq G$, then neither (i) nor (ii) holds. Now suppose that A generates G and show that assertions (i) and (ii) of the theorem are equivalent. One direction is easy: if (ii) holds, then Lemmata 5.1 and 5.4 show that $\operatorname{diam}_A(G) = \operatorname{diam}_B(G)$, as wanted.

Now suppose that (i) holds, that is $\operatorname{diam}_A(G) = \operatorname{diam}(G)$. We can assume that $A^{\pm} = A$. By Lemma 5.3, there is a standard generating set $B \subseteq A$.

To simplify the notation, we assume further that $G = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ where $1 < m_1 \mid \cdots \mid m_r$ and that $B = \{(1,0,\dots,0),\dots,(0,\dots,0,1)\}$. Let $g \in G$ with $l_A(g) = \operatorname{diam}(G) = \sum_{i=1}^{r} \lfloor m_i/2\rfloor$. Then certainly $l_B(g) = \sum_{i=1}^{r} \lfloor m_i/2\rfloor$, and so $g = (\lambda_1,\dots,\lambda_r)$ for suitable $\lambda_1,\dots,\lambda_r \in \mathbb{Z}$ with $|\lambda_i| = \lfloor m_i/2\rfloor$ for all $i \in [1,r]$.

Now suppose that $a = (\alpha_1,\dots,\alpha_r) \in A \setminus B^{\pm}$. Then a has at least two non-zero components. If it had more than two non-zero components, then $l_B(g+a)$ or $l_B(g-a)$ would be less than $l_B(g)-1$, a contradiction to $l_A(g) = l_B(g)$. So exactly two components of a are non-zero, say α_i and α_j where $i < j$.

Moreover, we must have $\alpha_i, \alpha_j \in \{-1,1\}$, because otherwise $l_B(g+a)$ or $l_B(g-a)$ would again be less than $l_B(g)-1$. Our next aim is to show that $m_i = m_j = 3$.

If one of m_i, m_j were even, then $l_B(g+a)$ or $l_B(g-a)$ would be less than $l_B(g)-1$, a contradiction. If m_i and m_j were both greater than 4, then $l_B(g+2a)$ or $l_B(g-2a)$ would be less than $l_B(g)-2$, impossible. If $m_i = 3$ and $m_j > 3$, then either one of $l_B(g+a)$, $l_B(g-a)$ would be less than $l_B(g)-1$ or one of $l_B(g+2a)$, $l_B(g-2a)$ would be less than $l_B(g)-2$, again a contradiction.

The only remaining possibility is $m_i = m_j = 3$, and in view of Lemma 5.1, we are reduced to the case where G is a homocyclic group of exponent 3. Now (ii) follows from Lemma 5.4. □

Proof of Corollary 2.3. We have to bound the size of $A \subseteq G$ satisfying $\operatorname{diam}_A(G) = \operatorname{diam}(G)$. For brevity, we write $\nu_2 := \nu_2(G)$, $\nu_3 := \nu_3(G)$, and $r := \operatorname{rk}(G)$. Since A generates G, we certainly have $r \leqslant |A|$, and it remains to show that $|A| \leqslant 1 + 2r - \nu_2 + 2\lfloor \nu_3/2\rfloor$.

Based upon Theorem 2.2, we pick a standard generating set $B = \{b_1,\dots,b_r\}$ for G such that

$$A \subseteq \bigl(B \cup \{b_{2i-1} + b_{2i}\colon\ i \in [1, \nu_3/2]\}\bigr)^{\pm}.$$

First suppose that $\nu_3 = 0$. Then we have $A \subseteq B^{\pm}$, and $B^{\pm}$ is the disjoint union of $\{0\}$, $\{b_i\colon\ i \in [1,\nu_2]\}$, $\{b_i\colon\ i \in [\nu_2+1, r]\}$, and $\{-b_i\colon\ i \in [\nu_2+1, r]\}$. This gives $|A| \leqslant 1 + \nu_2 + 2(r-\nu_2) = 1 + 2r - \nu_2$, as wanted.

Now suppose that $\nu_3 \neq 0$. Then $\nu_2 = 0$, and the set $(B \cup \{b_{2i-1} + b_{2i}\colon\ i \in [1,\nu_3/2]\})^{\pm}$ is the disjoint union of $\{0\}$, B, $-B$, $\{b_{2i-1} + b_{2i}\colon\ i \in [1,\nu_3/2]\}$, and $\{-(b_{2i-1} + b_{2i})\colon\ i \in [1,\nu_3/2]\}$. This gives $|A| \leqslant 1 + 2r + 2\lfloor \nu_3/2\rfloor$, completing the proof. □

6. The size of small diameter sets, I: First results

Let G be a finite Abelian group, and suppose that $\rho \in [2, \operatorname{diam}(G)]$. In this section we collect some general observations regarding the invariants $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$, and we determine them completely for $\rho = 2$. The assertions of Lemma 2.4, Example 2.5, Proposition 2.6, Corollary 2.8, and Proposition 2.11 will be proved.

We start with Lemma 2.4, explaining the relation between $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$.

Proof of Lemma 2.4. Recall that $\rho \in [2, \operatorname{diam}(G)]$. We have to show that

$$\mathbf{s}_\rho(G) = \max\bigl\{|H| \cdot \mathbf{t}_\rho(G/H):\ H \lneqq G\bigr\}.$$

Suppose that A is a ρ-maximal generating set for G, and write $H := \pi(A) \lneqq G$. Then the image $\overline{A}$ of A under the canonical homomorphism $G \to G/H$ is ρ-maximal in G/H, non-zero, and aperiodic; see the discussion in Section 2.2. We get $\mathbf{t}_\rho(G/H) \geqslant |\overline{A}| = |A|/|H|$, and if A is chosen so that $|A| = \mathbf{s}_\rho(G)$, this yields

$$\mathbf{s}_\rho(G) \leqslant |H| \cdot \mathbf{t}_\rho(G/H).$$

Conversely, let $H \lneqq G$ and suppose that $\overline{A}$ is an aperiodic ρ-maximal generating set for G/H. Let A denote the full pre-image of $\overline{A}$ in G under the canonical homomorphism $G \to G/H$. Then A is a generating set for G with $\operatorname{diam}_A(G) \geqslant \rho$. If $\overline{A}$ is chosen so that $|\overline{A}| = \mathbf{t}_\rho(G/H)$, we get

$$\mathbf{s}_\rho(G) \geqslant |A| = |H| \cdot \bigl|\overline{A}\bigr| = |H| \cdot \mathbf{t}_\rho(G/H). \qquad \square$$

In connection with the equation $\mathbf{t}_1(G) = 0$ it was indicated that $\mathbf{t}_\rho(G)$ may also vanish for certain $\rho \in [2, \operatorname{diam}(G)]$. Example 2.5 describes a situation of this kind.

Explanation of Example 2.5. Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n+1}}$ with $n \geqslant 2$. Theorem 2.1 shows that $\operatorname{diam}(G) = 1 + 2^n$. Let $A \subseteq G$ be maximal subject to $\langle A\rangle_{2^n-1} \neq \langle A\rangle = G$; we have to show that A is periodic.

By maximality, we have $A = A^{\pm}$. Since A generates G, there exists an element $a_1 \in A$ of order $\operatorname{ord}(a_1) = 2^{n+1}$, and furthermore there exists an element $a_2 \in A$ such that $a_2 \notin \langle a_1\rangle$. Without loss of generality, we may assume that $a_1 = (0,1)$ and $a_2 = (1,\alpha)$ with $0 \leqslant \alpha \leqslant 2^n$.

Notice that, whenever $(1,\beta) \in A$ (this holds for instance for $\beta = \alpha$), then

$$\begin{aligned} G \setminus \langle A\rangle_{2^n-1} &\subseteq (\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n+1}}) \setminus \langle (1,\beta), (0,1)\rangle_{2^n-1} \\ &\subseteq \bigl\{(0,2^n), (1,2^n-\beta), (1,2^n-1-\beta), (1,2^n+1-\beta)\bigr\}^{\pm}, \end{aligned} \tag{6.1}$$

and because $\langle A\rangle_{2^n-1} \neq G$, at least one of the elements $(0,2^n)$, $(1,2^n-\beta)$, $(1,2^n-1-\beta)$, $(1,2^n+1-\beta)$ has length greater than 2^n-1 with respect to A.

Assertion. *If* $b = (1, \beta) \in A$*, then* $b \in \{(1, 0), (1, 1), (1, 2^n - 1), (1, 2^n)\}^{\pm}$.

For a contradiction, suppose that $b = (1, \beta) \in A \setminus \{(1, 0), (1, 1), (1, 2^n - 1), (1, 2^n)\}^{\pm}$. Then we have $2b = (0, 2\beta) \notin \{(0, 0), (0, 1), (0, 2), (0, 3)\}^{\pm}$, and thus

$$\begin{aligned}
&(0, 2^n) - 2b = (0, 2^n - 2\beta) \in \langle a_1\rangle_{2^n-4}, &&\text{so } l_A(0, 2^n) \leqslant 2^n - 2;\\
&(1, 2^n - \beta) - b = (0, 2^n - 2\beta) \in \langle a_1\rangle_{2^n-4}, &&\text{so } l_A(1, 2^n - \beta) \leqslant 2^n - 3;\\
&(1, 2^n - 1 - \beta) - b = (0, 2^n - 1 - 2\beta) \in \langle a_1\rangle_{2^n-3}, &&\text{so } l_A(1, 2^n - 1 - \beta) \leqslant 2^n - 2;\\
&(1, 2^n + 1 - \beta) - b = (0, 2^n + 1 - 2\beta) \in \langle a_1\rangle_{2^n-3}, &&\text{so } l_A(1, 2^n + 1 - \beta) \leqslant 2^n - 2.
\end{aligned}$$

This contradicts the observation following (6.1).

Assertion. *If* $c = (0, \gamma) \in A$*, then* $c \in \{(0, 1)\}^{\pm}$.

Let $c = (0, \gamma) \in G \setminus \{(0, 1)\}^{\pm}$. Then it is easily seen that $\langle a_1, c\rangle_{2^n-2} = \{(0, \delta)\colon \delta \in \mathbb{Z}_{2^{n+1}}\}$, and hence $\langle a_1, a_2, c\rangle_{2^n-1} = G$. It follows that $c \notin A$, as required.

The two assertions above yield

$$\big\{(0, 1), (1, \alpha)\big\}^{\pm} \subseteq A \subseteq \big\{(0, 1), (1, 0), (1, 1), (1, 2^n - 1), (1, 2^n)\big\}^{\pm}.$$

Case 1: $(1, \alpha) = (1, 0)$. Because of (6.1) we certainly have $(1, 2^n - 1), (1, 2^n) \notin A$. On the other hand, $(0, 2^n) \notin \langle (0, 1), (1, 0), (1, 1)\rangle_{2^n-1}$. So $A = \{(0, 1), (1, 0), (1, 1)\}^{\pm}$ has non-trivial period $\{(0, 0), (1, 0)\}$.

Case 2: $(1, \alpha) = (1, 1)$. Again (6.1) shows that $(1, 2^n - 1), (1, 2^n) \notin A$. So as in in the first case $A = \{(0, 1), (1, 0), (1, 1)\}^{\pm}$ has non-trivial period $\{(0, 0), (1, 0)\}$.

Case 3: $(1, \alpha) \in \{(1, 2^n - 1), (1, 2^n)\}$. Write the elements of G with respect to the generating pair $((1, 2^n), (0, 1))$ rather than $((1, 0), (0, 1))$. In these new coordinates, a_1 is still represented by $(0, 1)$, but a_2 is represented by $(1, 0)$ or $(1, -1)$. We are reduced to either Case 1 or to Case 2. □

We now determine $\mathbf{t}_2(G)$ and $\mathbf{s}_2(G)$. Observe that $\mathrm{diam}(G) \geqslant 2$ if and only if $|G| > 3$ by Theorem 2.1.

Proof of Proposition 2.6. Let $A \subseteq G$. Then A is 2-maximal in G if and only if it has the form $A = G \setminus \{a, -a\}$ for some $a \in G \setminus \{0\}$. Furthermore we have $\pi(A) = \pi(G \setminus A)$, hence A is 2-maximal and aperiodic if and only if $A = G \setminus \{a, -a\}$ for some $a \in G$ with $\mathrm{ord}(a) \notin \{1, 4\}$.

Now, if $|G|$ is even, then $|G \setminus \{a, -a\}| = |G| - 1$ for every $a \in G$ with $\mathrm{ord}(a) = 2$. If $|G|$ is odd, then $|G \setminus \{a, -a\}| = |G| - 2$ for every $a \in G \setminus \{0\}$. □

Next we determine $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$ for $\rho = \mathrm{diam}(G)$.

Proof of Corollary 2.8. Recall that G is a finite Abelian group and $\rho = \mathrm{diam}(G) \geqslant 2$. Write $r := \mathrm{rk}(G)$. Then Corollary 2.3 shows that $\mathbf{s}_\rho(G) = 1 + 2r - \nu_2(G) + 2\lfloor \nu_3(G)/2 \rfloor$, and it remains to prove that $\mathbf{t}_\rho(G)$ has the same value.

In fact, Theorem 2.2 explains how to construct a ρ-maximal generating set for G: fix a standard generating set $B = \{b_1, \dots, b_r\}$, and put

$$A := \bigl(B \cup \{b_{2i-1} + b_{2i}\colon\ i \in [1, \nu_3(G)/2]\}\bigr)^{\pm}.$$

To conclude the proof we show that A is aperiodic.

For $r = 1$ the claim is clear. Now consider the case $r \geqslant 2$. First suppose that G is not homocyclic of exponent 3, or that r is odd. Then we have $(A + b_r) \cap A \subseteq \{0, b_r, -b_r\}$. So $\{-b_1, -b_r, 0\} \subseteq A$ implies that

$$\pi(A) \subseteq (A + b_1) \cap (A + b_r) \cap A = \{0\}.$$

Now suppose that G is a homocyclic group of exponent 3 and that r is even. Then by construction $|A| = 1 + 2r + r \equiv 1 \pmod 3$. As A is a union of $\pi(A)$-cosets, it follows that $\pi(A) = \{0\}$. $\square$

We end this section with two more lemmata and a proof of Proposition 2.11.

Lemma 6.1. *Let G be a finite Abelian group of odd order, and suppose that $\rho \in [2, \mathrm{diam}(G)]$. Then $\mathbf{s}_\rho(G)$ is odd, and $\mathbf{t}_\rho(G)$ is either zero or odd.*

Proof. Let A be a ρ-maximal subset of G. Then $A = A^{\pm}$, and since G contains no elements of order two, $|A| = |A^{\pm}|$ is odd. $\square$

Lemma 6.2. *Let A be a ρ-maximal subset of a finite Abelian group G, where $\rho \in [2, \mathrm{diam}(G)]$. Then $\pi(A) = \pi(\langle A \rangle_\tau)$ for all $\tau \in [1, \rho - 1]$.*

Proof. Clearly, we have $\pi(A) \subseteq \pi(\langle A \rangle_2) \subseteq \cdots \subseteq \pi(\langle A \rangle_{\rho-1})$. Write $H := \pi(\langle A \rangle_{\rho-1})$. Since

$$\langle A + H \rangle_{\rho-1} = \langle A \rangle_{\rho-1} + H = \langle A \rangle_{\rho-1} \subsetneqq G,$$

by maximality of A we have $A + H = A$, whence $H \subseteq \pi(A)$. $\square$

Proof of Proposition 2.11. Let A be a ρ-maximal aperiodic subset of G. By Lemma 6.2 we have $\pi(\langle A \rangle_\tau) = \{0\}$ for all $\tau \in [1, \rho - 1]$. So Kneser's theorem (Corollary 4.4) shows that

$$|G| - 1 \geqslant \bigl|\langle A \rangle_{\rho-1}\bigr| \geqslant (\rho - 1)|A| - (\rho - 2),$$

hence $|A| \leqslant (|G| - 2)/(\rho - 1) + 1$, proving the first assertion.

Note that the largest odd integer, not exceeding the right-hand side of this inequality, is $2\lfloor(|G|-2)/(2(\rho-1))\rfloor+1$. So, if $\mathrm{rk}_2(G)=0$, the second assertion follows from Lemma 6.1.

Finally, suppose that $\mathrm{rk}_2(G)=1$, and let g denote the unique element of order two in G. Put $k:=\lfloor(|G|-2)/(2(\rho-1))\rfloor$. By the above we have

$$|A|\leqslant\frac{|G|-2}{\rho-1}+1<2k+3,$$

and we need to show that in fact $|A|\leqslant 2k+1$.

For a contradiction, suppose that $|A|=2k+2$. Since $0\in A=A^{\pm}$ and since $|A|$ is even, we conclude that $g\in A$ and therefore $g\in\langle A\rangle_\tau$ for all $\tau\in[1,\rho-1]$. So for these values of τ the cardinalities $|\langle A\rangle_\tau|$ are even, too. By Lemma 6.2, the sets $\langle A\rangle_\tau$ are aperiodic, and Kneser's theorem implies

$$\bigl|\langle A\rangle_\tau\bigr|\geqslant\bigl|\langle A\rangle_{\tau-1}\bigr|+|A|-1\quad(\tau\in[1,\rho-1]).$$

Comparing the parities of the two sides (for each of these inequalities) we get

$$\bigl|\langle A\rangle_{\rho-1}\bigr|\geqslant\bigl|\langle A\rangle_{\rho-2}\bigr|+|A|\geqslant\cdots\geqslant(\rho-1)|A|=2(\rho-1)(k+1)>|G|-2.$$

Since $|\langle A\rangle_{\rho-1}|$ and $|G|$ are both even, we have $\langle A\rangle_{\rho-1}=G$, a contradiction. □

7. The size of small diameter sets, II: Cyclic groups

Let $G\cong\mathbb{Z}_m$ be the cyclic group of order m. According to Theorem 2.1 we have $\mathrm{diam}(G)=\lfloor m/2\rfloor$. In this section we prove Theorem 2.9, thus determining $\mathbf{t}_\rho(G)$ and $\mathbf{s}_\rho(G)$ for all $\rho\in[1,m/2]$.

Proof of Theorem 2.9. It suffices to show that

$$\mathbf{t}_\rho(\mathbb{Z}_m)=2\left\lfloor\frac{m-2}{2(\rho-1)}\right\rfloor+1;$$

the formula for $\mathbf{s}_\rho(\mathbb{Z}_m)$ then follows from Lemma 2.4.

Set $k:=\lfloor(m-2)/(2(\rho-1))\rfloor$, so that $k\geqslant 1$ in view of $\rho\leqslant m/2$ and

$$2(\rho-1)k+1\leqslant(m-2)+1<m. \tag{7.1}$$

By Proposition 2.11, we have $\mathbf{t}_\rho(\mathbb{Z}_m)\leqslant 2k+1$. Therefore, it suffices to exhibit a ρ-maximal aperiodic subset $A\subseteq\mathbb{Z}_m$ of cardinality $|A|\geqslant 2k+1$.

Put $B:=\{-k,-k+1,\dots,k\}$. Then (7.1) yields

$$\langle B\rangle_{\rho-1}=\bigl\{-(\rho-1)k,-(\rho-1)k+1,\dots,(\rho-1)k\bigr\}\neq\mathbb{Z}_m, \tag{7.2}$$

and we pick a ρ-maximal subset $A \subseteq \mathbb{Z}_m$ containing B. It is enough to show that A is aperiodic; in fact this will imply that $A = B$.

Writing $H := \pi(A)$, we observe that

$$\langle B\rangle_{\rho-1} + H \subseteq \langle A\rangle_{\rho-1} + H = \langle A\rangle_{\rho-1} \subsetneqq \mathbb{Z}_m$$

by Lemma 6.2. On the other hand, (7.2) shows that

$$\left|\langle B\rangle_{\rho-1}\right| = 2(\rho-1)k + 1 > 2(\rho-1)\frac{(m-2)}{4(\rho-1)} + 1 = m/2.$$

Thus $\langle B\rangle_{\rho-1} + H \subsetneqq \mathbb{Z}_m$ implies $H = \{0\}$, as claimed. $\square$

For later use we record separately the case $\rho = 3$.

Corollary 7.1. *For every $m \in \mathbb{N}$ with $m \geqslant 6$ we have*

$$\mathbf{t}_3(\mathbb{Z}_m) = 2\left\lfloor \frac{m-2}{4} \right\rfloor + 1,$$

and

$$\mathbf{s}_3(\mathbb{Z}_m) = \begin{cases} \dfrac{m-1}{2} - 1 & \textit{if } m \equiv 1 \pmod 4, \\ \dfrac{m-1}{2} & \textit{if } m \equiv 3 \pmod 4, \\ \dfrac{m}{2} - 1 & \textit{if } m \textit{ is a power of } 2, \\ \dfrac{m}{2} & \textit{otherwise.} \end{cases}$$

Proof. The expression for $\mathbf{t}_3(\mathbb{Z}_m)$ comes directly from Theorem 2.9, which also yields

$$\mathbf{s}_3(\mathbb{Z}_m) = \frac{m}{2} - \min\left\{ \frac{2m}{d}\left\{\frac{d-2}{4}\right\} \colon d \mid m, d \geqslant 6 \right\}, \tag{7.3}$$

where $\{x\} := x - \lfloor x \rfloor$ denotes the fractional part of $x \in \mathbb{R}$.

If $m = 2^k n$ with $n, k \in \mathbb{N}$ and $n \geqslant 3$ odd, then the minimum on the right hand side of (7.3) is attained for $d = 2n \equiv 2 \pmod 4$.

If $m = 2^k$ with an integer $k \geqslant 3$, then $\{(d-2)/4\} = 1/2$ for any $d \mid m, d \geqslant 6$; therefore the minimum is attained for $d = m$.

If $m \equiv 3 \pmod 4$, then $\{(d-2)/4\} \geqslant 1/4 = \{(m-2)/4\}$; again, the minimum is attained for $d = m$.

Finally, suppose that $m \equiv 1 \pmod 4$. If $d \mid m$ and $d \equiv 1 \pmod 4$, then

$$\frac{2m}{d}\left\{\frac{d-2}{4}\right\} \geqslant \frac{2m}{m}\left\{\frac{m-2}{4}\right\} = \frac{3}{2}.$$

If $d \mid m$ and $d \equiv 3 \pmod 4$, then $d \leqslant m/3$, and so we have

$$\frac{2m}{d}\left\{\frac{d-2}{4}\right\} \geqslant \frac{2m}{m/3}\frac{1}{4} = \frac{3}{2}.$$

The minimum, once again, is attained for $d = m$. $\square$

8. The size of small diameter sets, III: Sets of diameter 3

Let G be a finite Abelian group. In this section we determine $\mathbf{t}_3(G)$ and $\mathbf{s}_3(G)$, proving Theorem 2.7.

Lemma 8.1. *Let G be a finite Abelian group and let $H \leqslant G$. Then for every $\rho \in [1, \operatorname{diam}(G/H)]$ we have $\mathbf{s}_\rho(G) \geqslant |H| \cdot \mathbf{s}_\rho(G/H)$. In particular,* $\operatorname{diam}(G) \geqslant \operatorname{diam}(G/H)$.

Proof. Given $\rho \in [1, \operatorname{diam}(G/H)]$, we choose a generating subset $\overline{A} \subseteq G/H$ such that $\operatorname{diam}_{\overline{A}}(G/H) \geqslant \rho$ and $|\overline{A}| = \mathbf{s}_\rho(G/H)$. Let $A \subseteq G$ denote the full pre-image of $\overline{A}$ under the canonical homomorphism $G \to G/H$. Then A is a generating subset of G with $\operatorname{diam}_A(G) \geqslant \rho$ and $|A| = |H| \cdot |\overline{A}| = |H| \cdot \mathbf{s}_\rho(G/H)$; cf. the discussion in Section 2.2. $\square$

Lemma 8.2. *Let G be a finite Abelian group with* $\operatorname{diam}(G) \geqslant 3$. *Then*

$$\mathbf{s}_3(G) \leqslant \frac{|G|}{2}.$$

Moreover, if $|G|$ is odd and $n := \exp(G)$, then

$$\mathbf{s}_3(G) \leqslant \begin{cases} \dfrac{n-1}{2n}|G| - 1 & \text{if } n \equiv 1 \pmod 4, \\ \dfrac{n-1}{2n}|G| & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Proof. The first assertion is immediate from the boxing principle: if $A \subseteq G$ satisfies $|A| > |G|/2$, then $\langle A\rangle_2 = 2A^{\pm} = G$.

Now suppose that $|G|$ is odd. Let A be a generating subset with $\operatorname{diam}_A(G) \geqslant 3$. Fix $z \in G \setminus \langle A\rangle_2$ and write $d := \operatorname{ord}(z)$. Since $z \notin A - A$, for every $g \in G$ at least one of the elements g and $g + z$ does not belong to A. Thus every $\langle z\rangle$-coset in G contains at most $(d-1)/2$ elements of A, and therefore

$$|A| \leqslant \frac{d-1}{2}\frac{|G|}{d} \leqslant \frac{n-1}{2n}|G|.$$

The second assertion now follows from Lemma 6.1. $\square$

Lemma 8.3. *Let G be a non-trivial finite Abelian group.*

(i) *Suppose that* $\mathrm{rk}_2(G) = 0$. *Then there exists an aperiodic subset $A \subseteq G$ such that* $|A| = (|G| - 1)/2$ *and* $0 \notin 2A$.
(ii) *Suppose that* $\mathrm{rk}_2(G) > \mathrm{rk}_2(2 * G)$ *and* $G \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. *Then* $\mathbf{t}_3(G) \geqslant |G|/2$.
(iii) *Suppose that* $\mathrm{rk}_2(G) = \mathrm{rk}_2(2 * G) \geqslant 1$ *and* $\exp(G) > 4$. *Then* $\mathbf{t}_3(G) \geqslant |G|/2 - 1$.

Proof. (i) As G contains no elements of order two, $G \setminus \{0\}$ is the disjoint union of 2-subsets of the form $\{g, -g\}$ ($g \in G \setminus \{0\}$). Suppose that $A \subseteq G$ contains exactly one element from each of these 2-subsets. Then it is immediate that $|A| = (|G| - 1)/2$ and $0 \notin 2A$. Since $\gcd(|G|, |A|) = 1$, the set A is aperiodic; see Section 2.2.

(ii) Fix an element $h \in G$ with $\mathrm{ord}(h) = 2$ and a subgroup $K \leqslant G$ such that $G = K \oplus \langle h\rangle$. Put $A := \{0\} \cup (K + h) \setminus \{h\}$. As $|A| = |G|/2$, it suffices to show that A is 3-maximal and aperiodic. The former follows from the first part of Lemma 8.2 and $\langle A\rangle_2 = G \setminus \{h\}$. This also yields $\pi(A) \subseteq \pi(\langle A\rangle_2) = \pi(G \setminus \langle A\rangle_2) = \pi(\{h\}) = \{0\}$.

(iii) Fix an element $h \in G$ of order $\mathrm{ord}(h) > 4$ and a subgroup $K \leqslant G$ of index $[G : K] = 2$ so that $G = K + \langle h\rangle$. Put $A := \{0\} \cup (K + h) \setminus \{h, -h\}$. Evidently, we have $|A| = |G|/2 - 1$. Since $|G|$ is divisible by four, we obtain $\gcd(|G|, |A|) = \gcd(2, |G|/2 - 1) = 1$. Therefore A is aperiodic; see Section 2.2.

It remains to show that A is 3-maximal. For this we observe that $\langle A\rangle_2 = G \setminus \{h, -h\}$. For a contradiction, suppose that there exists $g \in G \setminus A$ satisfying $\langle \{g\} \cup A\rangle_2 \neq G$. Then $g \in K \setminus \{0\}$, and $h - g, h + g \notin A$. This implies that $h - g = -h = h + g$, hence $4h = 2g = 0$, a contradiction. □

Lemma 8.4. *Let G be a non-cyclic finite Abelian group of odd order with* $\mathrm{diam}(G) \geqslant 3$. *Writing $n := \exp(G)$, we have*

$$\mathbf{t}_3(G) = \begin{cases} \dfrac{n-1}{2n}|G| - 1 & \text{if } n \equiv 1 \pmod 4, \\ \dfrac{n-1}{2n}|G| & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Proof. In view of Lemma 8.2, it suffices to construct an aperiodic generating set A for G of diameter $\mathrm{diam}_A(G) \geqslant 3$ and appropriate size.

Since G is not cyclic, we may assume that $G = H \oplus \mathbb{Z}_n$ where $\{0\} \neq H \leqslant G$. Elements of G will be written as pairs (h, x) with $h \in H$ and $x \in \mathbb{Z}_n$.

By Lemma 8.3(i), there exists an aperiodic subset $B \subseteq H$ of cardinality $|B| = (|H| - 1)/2$ such that $0 \notin 2B$, and all the more so, $0 \notin B$. Put $k := \lfloor n/4 \rfloor$ so that $k \geqslant 1$, unless $n = 3$ (in which case G is homocyclic of exponent 3).

If $n = 4k + 1$, we define

$$\begin{aligned} A := {} & \bigl(H + \bigl\{(0, -k+1), (0, -k+2), \ldots, (0, k-2), (0, k-1)\bigr\}\bigr) \\ & \cup \bigl(B + \{(0, k)\}\bigr) \cup \bigl(-B - \{(0, k)\}\bigr). \end{aligned}$$

If $n = 4k + 3 \geqslant 7$, we define

$$\begin{aligned} A := {} & \bigl(H + \bigl\{(0, -k+1), (0, -k+2), \dots, (0, k-2), (0, k-1)\bigr\}\bigr) \\ & \cup \bigl(B + \bigl\{(0, k), (0, k+1)\bigr\}\bigr) \cup \bigl(-B - \{(0, k), (0, k+1)\}\bigr) \\ & \cup \bigl\{(0, k), (0, -k)\bigr\}. \end{aligned}$$

Finally, if $n = 3$, we define

$$A := \bigl(B + \{(0, 1)\}\bigr) \cup \bigl(-B - \{(0, 1)\}\bigr) \cup \{(0, 0)\}.$$

We have $\pi(A) = 0$. Indeed, if $n \neq 3$, then projecting onto the second coordinate shows that $\pi(A) \subseteq H$, and thus $\pi(A) \subseteq \pi(B) = \{0\}$. If $n = 3$, it is likewise easy to see that $\pi(A) \subseteq H$ and thus $\pi(A) \subseteq \pi(B) = \{0\}$.

Moreover, it is easily verified that $\langle A\rangle = G$ and $\operatorname{diam}_A(G) \geqslant 3$: the latter follows from

$$\langle A\rangle_2 \not\ni \begin{cases} (0, 2k) & \text{if } n = 4k + 1, \\ (0, 2k+1) & \text{if } n = 4k + 3. \end{cases}$$

Finally, we count

$$|A| = \begin{cases} (2k-1)|H| + 2|B| = 2k|H| - 1 & \text{if } n = 4k + 1, \\ (2k-1)|H| + 4|B| + 2 = (2k+1)|H| & \text{if } n = 4k + 3 \geqslant 7, \\ 2|B| + 1 = |H| & \text{if } n = 3. \end{cases}$$

Noticing that $|H| = |G|/n$ we get

$$|A| = \begin{cases} \dfrac{n-1}{2n}|G| - 1 & \text{if } n \equiv 1 \pmod 4, \\ \dfrac{n-1}{2n}|G| & \text{if } n \equiv 3 \pmod 4. \end{cases} \qquad \square$$

Lemma 8.5. *Let G be a finite Abelian group with* $\operatorname{diam}(G) \geqslant 3$ *and* $\operatorname{rk}_2(G) > \operatorname{rk}_2(2 * G)$. *Then* $\mathbf{t}_3(G) = \mathbf{s}_3(G) = |G|/2$.

Proof. Lemma 8.2 shows that $\mathbf{t}_3(G) \leqslant \mathbf{s}_3(G) \leqslant |G|/2$, while by Lemma 8.3(ii) we have $\mathbf{t}_3(G) \geqslant |G|/2$. $\square$

Lemma 8.6. *Let G be a finite Abelian group and let $A \subseteq G$. Suppose that $2 * G \nsubseteq \langle A\rangle_2$. Then*

$$|A| \leqslant \bigl(|G| - 2^{\operatorname{rk}_2(G)}\bigr)/2.$$

Proof. Fix $g \in G$ such that $2g \notin \langle A\rangle_2$, and put $X := \{x \in G\colon 2x = 0\}$. Then the sets $A - g$, $A + g$, and X are pairwise disjoint, whence

$$|A| \leqslant \bigl(|G| - |X|\bigr)/2 = \bigl(|G| - 2^{\operatorname{rk}_2(G)}\bigr)/2. \qquad \square$$

Lemma 8.7. *Let G be a finite Abelian group with* $\mathrm{rk}_2(G) = \mathrm{rk}_2(2*G) \geqslant 1$ *and* $\exp(G) > 4$. *Then we have* $\mathbf{t}_3(G) = |G|/2 - 1$.

Proof. In view of Lemmata 8.2 and 8.3(iii), it suffices to show that $\mathbf{t}_3(G) \neq |G|/2$. For a contradiction, suppose that A is a 3-maximal aperiodic subset of G of cardinality $|A| = |G|/2$. Kneser's theorem and Lemma 6.2 show that $|\langle A\rangle_2| = |G| - 1$, so $\langle A\rangle_2 = G \setminus \{h\}$ for some $h \in \{x \in G\colon 2x = 0\} \subseteq 2*G$. Now by Lemma 8.6 we have $|A| \leqslant (|G| - 2)/2 = |G|/2 - 1$, a contradiction. □

Lemma 8.8. *Let $G = \mathbb{Z}_4 \oplus \cdots \oplus \mathbb{Z}_4$ be a homocyclic group of exponent* 4 *and rank $r \geqslant 2$. Suppose that $A \subseteq G$ is a* 3*-maximal subset such that $(2*G) \cup \langle A\rangle_2 \neq G$. Then A is periodic.*

Proof. Choose $h \in G \setminus ((2*G) \cup \langle A\rangle_2)$, so that in particular $\mathrm{ord}(h) = 4$. We claim that $2h \in \pi(A)$. Indeed, it is enough to show that $a + 2h \in A$ for any given $a \in A$, and since A is 3-maximal this will follow from $h \notin \langle A \cup \{a + 2h\}\rangle_2$.

Since $h \notin 2*G$, we have $h \neq 2(a + 2h)$. Since $a \in A$ and $h \notin \langle A\rangle_2$, we have $h - (a + 2h) = -a - h \notin A$ and $h + (a + 2h) = a - h \notin A$. This shows that $h \notin \langle A \cup \{a + 2h\}\rangle_2$. □

Lemma 8.9. *Let $G = \mathbb{Z}_4 \oplus \cdots \oplus \mathbb{Z}_4$ be a homocyclic group of exponent* 4 *and rank $r \geqslant 2$. Then* $\mathbf{t}_3(G) = (|G| - \sqrt{|G|})/2 = (4^r - 2^r)/2$.

Proof. From Lemmata 8.6 and 8.8 it follows that $\mathbf{t}_3(G) \leqslant (|G| - 2^{\mathrm{rk}_2(G)})/2 = (4^r - 2^r)/2$. Thus, it remains to construct a 3-maximal aperiodic subset $A \subseteq G$ of size $|A| = (4^r - 2^r)/2$. We use induction on r.

If $r = 2$, then $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$, and we define

$$A := \big\{(k, 0)\colon k \in \mathbb{Z}_4\big\} \cup \big\{(1, 1), (-1, -1)\big\}.$$

Here $|A| = 6 = (16 - 4)/2$, and it is readily checked that A is a 3-maximal aperiodic subset of G. Indeed, we have $\langle A\rangle_2 = G \setminus \{(0, 2), (1, 2), (-1, 2)\}$.

Now suppose that $r \geqslant 3$. We write $G = H \oplus \mathbb{Z}_4$, where H is a homocyclic group of exponent 4 and rank $r - 1$. By the induction hypothesis, there exists a 3-maximal aperiodic subset $B \subseteq H$ with $|B| = (4^{r-1} - 2^{r-1})/2$. Put

$$A := \big\{(h, 0)\colon h \in H\big\} \cup \big\{(b, 1)\colon b \in B\big\} \cup \big\{(-b, -1)\colon b \in B\big\}.$$

Then $|A| = |H| + 2|B| = 4^{r-1} + 4^{r-1} - 2^{r-1} = (4^r - 2^r)/2$, and it is readily checked that A is 3-maximal and aperiodic. Indeed, we have $\langle A\rangle_2 = G \setminus \{(h, 2)\colon h \notin \langle B\rangle_2\}$. □

Lemma 8.10. *Let G be a finite Abelian group. Suppose that G is not cyclic and* $\mathrm{rk}_2(G) = \mathrm{rk}_2(2*G) \geqslant 1$. *Then* $\mathbf{s}_3(G) = |G|/2$.

Proof. First suppose that $\mathrm{rk}_2(G) = 1$. Then we can write $G = H \oplus \mathbb{Z}_m$, where m is even and not a power of 2. By Lemmata 8.2 and 8.1 and Corollary 7.1 we have

$$|G|/2 \geqslant \mathbf{s}_3(G) \geqslant |H| \cdot \mathbf{s}_3(\mathbb{Z}_m) = |G|/2,$$

and the claim follows.

Now suppose that $\mathrm{rk}_2(G) \geqslant 2$. In this case we find $H \leqslant G$ such that $G/H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$. Considering the set $A = \{(0,0), (1,0), (0,1), (0,3)\} \subseteq \mathbb{Z}_2 \oplus \mathbb{Z}_4$, one concludes easily that $\mathbf{s}_3(\mathbb{Z}_2 \oplus \mathbb{Z}_4) \geqslant 4$, and the proof can be completed as above. $\square$

Proof of Theorem 2.7. (i) Suppose that $|G|$ is odd. If G is cyclic, the assertion follows from Corollary 7.1. If G is not cyclic, the assertion follows from Lemmata 8.2 and 8.4.

(ii) Suppose that $|G|$ is even. If G is cyclic, the assertion follow from Corollary 7.1. Now suppose that G is not cyclic. Then the claim regarding $\mathbf{t}_3(G)$ follows from Lemmata 8.5, 8.7, and 8.9. Finally, the claim regarding $\mathbf{s}_3(G)$ follows from Lemmata 8.5 and 8.10. $\square$

9. The size of small diameter sets, IV: General estimates

In this section we prove Theorems 2.12 and 2.13.

Proof of Theorem 2.12. It suffices to show that $\mathbf{s}_\rho(G) \leqslant \frac{3}{2}\rho^{-1}|G|$ and that (i) implies (ii). Indeed, (ii) trivially implies (i), and it is easily seen that, if (i) and (ii) are equivalent, then equality holds in $\mathbf{s}_\rho(G) \leqslant \frac{3}{2}\rho^{-1}|G|$ if and only if G has a subgroup H such that G/H is cyclic of order 2ρ.

Let A be a generating set for G with $\mathrm{diam}_A(G) \geqslant \rho$. We write $H := \pi(\langle A\rangle_{\rho-1})$ and note that both G and $\langle A\rangle_{\rho-1}$ are unions of H-cosets, whence $|G| \geqslant |\langle A\rangle_{\rho-1}| + |H|$. Since

$$\langle A\rangle_{\rho-1} = (\rho-1)A^{\pm} + H = (\rho-1)\bigl(A^{\pm} + H\bigr),$$

Kneser's theorem yields

$$\bigl|\langle A\rangle_{\rho-1}\bigr| \geqslant (\rho-1)\bigl|A^{\pm} + H\bigr| - (\rho-2)|H|.$$

Combining these observations, we obtain

$$|G| \geqslant (\rho-1)\bigl|A^{\pm} + H\bigr| - (\rho-3)|H|. \tag{9.1}$$

Since $0 \in A^{\pm} \nsubseteq H$, the set $A^{\pm} + H$ is the union of at least two H-cosets. Moreover, if $A^{\pm}$ were the union of *exactly two* H-cosets, then $A^{\pm} + H = H \cup (g + H)$ for some $g \in G \setminus H$ satisfying $g + H = -g + H$, and hence $2g \in H$. But this would yield

$$G = \bigl\langle A^{\pm}\bigr\rangle \subseteq \bigl\langle A^{\pm} + H\bigr\rangle = H \cup (g + H) = (\rho-1)\bigl(A^{\pm} + H\bigr) = \langle A\rangle_{\rho-1} \subsetneqq G,$$

a contradiction.

We conclude that $A^{\pm} + H$ consists of at least three H-cosets, and so $|A^{\pm} + H| \geqslant 3|H|$. From (9.1) we obtain

$$|G| \geqslant \left(\rho - 1 - \frac{1}{3}(\rho - 3)\right)\left|A^{\pm} + H\right| \geqslant \frac{2}{3}\rho|A|. \tag{9.2}$$

This gives the upper bound $\mathbf{s}_\rho(G) \leqslant \frac{3}{2}\rho^{-1}|G|$; it remains to show that (i) implies (ii).

To this end, in addition to our earlier assumption that A is a generating set for G with $\operatorname{diam}_A(G) \geqslant \rho$, we assume that $|A| = \frac{3}{2}\rho^{-1}|G|$. Then (9.2) yields $A = A^{\pm} + H$, and this set is the union of exactly three H-cosets. Consequently, there are two possibilities: either $A = H \cup (g_1 + H) \cup (g_2 + H)$, where $g_1 + H, g_2 + H \in G/H$ are distinct elements of order two, or $A = (-g + H) \cup H \cup (g + H)$, where $g + H \in G/H$ is of order greater than two. In the first case we would have

$$G = \langle A\rangle = \{0, g_1, g_2, g_1 + g_2\} + H = \langle A\rangle_{\rho-1} \subsetneqq G,$$

a contradiction. Thus we are left with the second case: $A = (-g + H) \cup H \cup (g + H)$, where $g + H \in G/H$ has order strictly greater than two.

Since A generates G, the quotient group G/H is cyclic and generated by $g + H$. Since

$$\bigcup\{kg + H\colon -\rho + 1 \leqslant k \leqslant \rho - 1\} = \langle A\rangle_{\rho-1} \subsetneqq G,$$

the order of G/H is at least 2ρ. As $|A| = \frac{3}{2}\rho^{-1}|G|$, the estimate

$$|A| = 3|H| = 3\frac{|G|}{|G/H|} \leqslant 3\frac{|G|}{2\rho} = |A|$$

yields $|G/H| = 2\rho$, as desired. $\square$

Proof of Theorem 2.13. Let $A \subseteq G$ be a generating set such that $\operatorname{diam}_A(G) \geqslant \rho$ and $|A^{\pm}| > 4|G|/(3\rho - 1)$. We set $H := \pi(\langle A\rangle_{\rho-1})$ and show that there exists $g \in G$ such that

(i) $A \subseteq (-g + H) \cup H \cup (g + H)$, and $|A^{\pm}| > (3 - (\rho - 3)/(3\rho - 1))|H|$;
(ii) G/H is cyclic of order $2\rho \leqslant |G/H| \leqslant \frac{9}{4}\rho - 1$, and $g + H$ generates G/H.

As in the proof of Theorem 2.12 we see that $A^{\pm} + H$ consists of three H-cosets: the possibility $|A^{\pm} + H| \geqslant 4|H|$ is ruled out, since otherwise

$$|G| \geqslant \left(\rho - 1 - \frac{1}{4}(\rho - 3)\right)\left|A^{\pm} + H\right| \geqslant \frac{3\rho - 1}{4}\left|A^{\pm}\right|,$$

contrary to the assumptions. Exactly as before, the quotient group G/H is cyclic of order at least 2ρ, and there exists $g \in G$ such that $g + H$ is a generator of G/H and $A^{\pm} + H = (-g + H) \cup H \cup (g + H)$.

Finally, from

$$3|H| = \left|A^{\pm} + H\right| \geqslant \left|A^{\pm}\right| > 4|H||G/H|/(3\rho - 1)$$

it follows that $|G/H| \leqslant \frac{9}{4}\rho - 1$, and from

$$\left|A^{\pm}\right| > |H| \frac{4|G/H|}{3\rho - 1} \geqslant |H| \frac{8\rho}{3\rho - 1}$$

we obtain $|A^{\pm}| > (3 - (\rho - 3)/(3\rho - 1))|H|$, as required. $\square$

In fact one can go further and, given $\varepsilon > 0$, describe in a similar way the structure of those generating sets A for G which satisfy $\mathrm{diam}_A(G) \geqslant \rho$ and $|A^{\pm}| > (1+\varepsilon)|G|/(\rho - 1)$. Indeed, in this case $A^{\pm} + H$ consists of at most $\lceil \varepsilon^{-1} \rceil$ H-cosets. However, for small ε the description is likely to become quite complicated.

Acknowledgment

We thank the referee for the careful reading of our manuscript and the suggestions which led to a number of improvements in the exposition.

References

[1] L. Babai, G. Hetyei, W.M. Kantor, A. Lubotzky, Á. Seress, On the diameter of finite groups, in: Proc. of 31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, 22–24 October 1990, Vol. II, IEEE Computer Society Press, 1990, pp. 857–865.
[2] A. Bruen, L. Haddad, D. Lucien, Binary codes and caps, J. Combin. Des. 6 (4) (1998) 275–284.
[3] W.E. Clark, J. Pedersen, Sum-free sets in vector spaces over GF(2), J. Combin. Theory Ser. A 61 (2) (1992) 222–229.
[4] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering Codes, in: North-Holland Mathematical Library, Vol. 54, North-Holland, Amsterdam, 1997.
[5] G. Cohen, G. Zémor, Subset sums and coding theory, in: J.-M. Deshouillers, et al. (Eds.), Structure Theory of Set Addition, in: Astérisque, Vol. 258, Société Mathématique de France, Paris, 1999, pp. 327–339.
[6] A.A. Davydov, L.M. Tombak, Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry, Problemy Peredachi Informatsii 25 (4) (1989) 11–23 (in Russian); Transl. Problems Inform. Transmission 25 (4) (1989) 265–275.
[7] G. Faina, F. Pambianco, On the spectrum of the values k for which a complete k-cap in $\mathrm{PG}(n, q)$ exists, J. Geom. 62 (1–2) (1998) 84–98.
[8] Y.O. Hamidoune, Ö.J. Rödseth, On bases for σ-finite groups, Math. Scand. 78 (2) (1996) 246–254.
[9] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, Math. Z. 58 (1953) 459–484.
[10] M. Kneser, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, Math. Z. 61 (1955) 429–434.
[11] V.F. Lev, Generating binary spaces, J. Combin. Theory Ser. A, to appear.
[12] H.B. Mann, Addition Theorems: The Addition Theorems of Group Theory and Number Theory, Interscience Publishers/Wiley, New York, 1965.
[13] G. Zémor, Subset sums in binary spaces, European J. Combin. 13 (3) (1992) 221–230.